

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

Christopher George Pable	)	
	)	
Plaintiff/Counter-	)	
Defendant,	)	
	)	
	)	
	)	
	)	
v.	)	No. 19-cv-7868
	)	
Chicago Transit Authority and	)	
Clever Devices, Ltd.	)	
	)	
Defendants/Counter-	)	
Plaintiffs.	)	

Memorandum Opinion and Order

Plaintiff Christopher Pable worked for defendant Chicago Transit Authority ("CTA") as a computer programmer and analyst from May 7, 2012, through November 8, 2018, when he resigned in lieu of termination. A previous order in this case summarized the events leading up to his resignation as follows:

[Pable] and his supervisor Michael Haynes ("Haynes") discovered a "Skeleton Key" in the CTA's BusTime system, an application that provides alerts and service information to public transit users. The Skeleton Key was a flaw in the BusTime application that could allow an unauthorized user to take control of the application and post unauthorized alerts on the system. Pable alleges that he urged Haynes to report the flaw to the CTA, but Haynes wanted to test whether it was in fact possible to gain control of the BusTime application using the Skeleton Key.

In doing so, Haynes posted an alert on the BusTime system being used in Dayton, Ohio, which automatically posted that alert to Dayton's public Twitter account. After an investigation, the CTA determined that Pable's actions violated multiple CTA rules, policies, and procedures, warranting his termination. Pable chose to resign instead of being fired.

*Pable v. Chicago Transit Auth.*, No. 19 CV 7868, 2021 WL 4789023, at \*1 (N.D. Ill. Apr. 2, 2021) (McShain, MJ). This action followed, in which plaintiff asserts a whistleblower claim under the National Transit Systems Security Act, 6 U.S.C. § 1142.

Defendant CTA filed a counterclaim alleging that "without authorization and/or by exceeding authorized access," plaintiff violated the Computer Fraud & Abuse Act, 18 U.S.C. § 1030, et seq. (the "CFAA"), by obtaining unauthorized control over the BusTime application and by encrypting his work computer without CTA's knowledge or approval. Pable moves for judgment on the pleadings as to this counterclaim, arguing that CTA's legal theory is foreclosed by *Van Buren v. United States*, 141 S. Ct. 1648 (2021). I agree and grant Pable's motion for the reasons below.

The CFAA punishes, among other things, the use or transmission of information obtained "without authorization or exceeding authorized access." 18 U.S.C.A. § 1030(a). *Van Buren* holds that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or

databases—that are off limits to him,” 141 S. Ct. 1648, 1662, but does not violate the statute by information the individual was authorized to access for an “improper purpose,” *id.* Here, the CTA acknowledges that Pable “accessed the Computer with the CTA’s authorization” but argues that “he exceeded that authorized access when he altered information on the Computer by encrypting its Primary Drive and installing and encrypting the Secondary Drive.” Resp., ECF 120 at 7 (emphasis in original). In other words, the CTA claims that Pable misused his authorized access for an improper purpose. That is precisely the type of claim that *Van Buren* held was outside the CFAA’s scope.

The CTA seeks to avoid this conclusion by arguing that the “scope of access to the device” was different in this case than in *Van Buren*. Specifically, the CTA contends that although “it gave Pable access to the Computer that had the Primary Drive on it for his job,” its “grant of access did not include authorization to either unilaterally encrypt the Primary Drive, or unilaterally install and encrypt the Secondary Drive, *for any purpose.*” *Id.* (emphasis in original). It is true that the CTA’s claim is a shade different from the claim in *Van Buren*, where the government alleged that a police officer abused the CFAA by running a license plate search in a state law enforcement database—something he was authorized to do in the course of his job duties—for “personal use” in violation of the police department policy. 141 S. Ct. at

1653. But the CTA offers neither argument nor authority to suggest that the distinction it highlights has any legal significance. *Van Buren*'s essential holding is that determining whether a user's conduct violates the CFAA requires a "gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1649. The CTA does not allege that the gates were "down" to Pable with respect to any area of its computer system. Instead, it alleges that he accessed the system through gates that were "up" to him, and that once inside, he took actions prohibited by the CTA's "rules, regulations, and policies." Compl. at ¶ 20. That claim falls squarely within *Van Buren*'s purview.

That the CTA also asserts a "transmission claim" does not alter the analysis. The allegation the CTA points to is that Pable "intentionally accessed the Computer and damaged and caused loss to it, including by...intentionally transmitting a command or code into the unauthorized encryption mechanism that Pable knew would cause the information needed to decrypt the Secondary Drive to be deleted in order to prevent the CTA from accessing its contents." Compl. at ¶ 34. The CTA suggests, without authority, that this allegation raises a distinct claim from the unauthorized access claim that *Van Buren* forecloses. There are at least two problems with this argument.

First, the language of the statute indicates that prohibited "transmissions" are those of "information" that a user has obtained through unauthorized access. See 18 U.S.C.A. § 1030(a) ("Whoever...having knowingly accessed a computer without authorization or exceeding authorized access, and *by means of such conduct having obtained information...*transmits, or causes to be communicated, delivered, or transmitted...*the same* to any person not entitled to receive it...shall be punished as provided in subsection (c) of this section."). This suggests that a transmission claim is a species of unauthorized access claim, not an independently actionable claim for the transmission of information that a user has obtained in a manner that does not violate the statute.


Second, the specific "transmission" the CTA complains of does not allege that Pable transmitted any "information," however obtained, to "any person not authorized to receive it." Instead, the CTA claims that Pable is subject to punishment under the CFAA for transmitting "a command or code," into some "mechanism" he created to encrypt a drive on the CTA's system and to install and encrypt a second drive on that system. But the CTA does not claim that Pable transmitted (or attempted to transmit) the "command or code" to "any person" or allowed any unauthorized person to access the encrypted drives or to receive information they contained. In short, Pable's alleged conduct may have violated the CTA's "rules,

regulations, and policies," Compl. at ¶ 20, but nothing on the face of the Complaint suggests that it amounts to the type of unlawful transmission the CFAA prohibits.

The CTA's final argument is that factual disputes prevent judgment in Pable's favor. But as Pable notes, the standard for judgment under Rule 12(c) *assumes* that the non-movant, i.e., the CTA, could prove the facts it alleges. See *Alexander v. City of Chicago*, 994 F.2d 333, 336 (7th Cir. 1993). Here, that means that I assume Pable used information he was authorized to access in ways prohibited by the CTA's "rules, regulations, and policies." For the reasons explained above, those facts do not state an actionable CFAA claim in light of *Van Buren*.

For the foregoing reasons, Pable's motion for judgment on the pleadings of the CTA's counterclaim is granted.

**ENTER ORDER:**

  
**Elaine E. Bucklo**  
United States District Judge

Dated: July 18, 2022